知彼知己 - 資安篇

森美力 (Samiux) 編著

二零一七年八月廿八日　第一版
二零一八年九月九日　修訂版
二零一八年十月廿九日　修訂二版

本書是在安卓 (Android) 手機利用 Google Docs 軟件完成。頁面是 B5 大小。

本書是免費版本，可以在我的個人網站 (https://www.infosec-ninjas.com) 下載。歡迎在你的親戚朋友之間轉閱，更歡迎將其翻譯成其他國家語言。

雖然是免費版本，但版權仍然歸於本人。

目錄

前言

孫子兵法有云 ：「知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。」 孫子兵法又云 ：「兵者，詭道也。故能而示之不能，用而示之不用，近而示之遠，遠而示之近。」

惡意黑客網絡攻防尤如戰場，可是互聯網並不是一個虛擬戰場，其實她是一個名符其實的真實戰場。全世界的軍事部門都有其網絡戰爭部隊來對應未來可能發生的網絡戰爭。

我們日常生活中的很多設備或設施都會接駁到互聯網，例如核電廠、發電廠、金融市場平台及通訊系統等等。如果這些設備被網絡攻擊，其後果亦不容忽視的。

作為互聯網的使用者，我們每日都要面對這個戰場。如何做到知道惡意黑客的攻擊，又知道自己的強項和弱點，而達到「知彼知己」的境地是何等的高興。

本書將會討論如何做到「知彼知己」，從認識惡意黑客的攻擊到認識自己的弱點上都會討論到。希望各位閱讀後有所得益和啓發。

雖然，本人力求做到盡善盡美，但其中難免有所錯漏，歡迎讀者指正與交流！

森美力 (Samiux) (網名)
寫於二零一七年八月廿六日，中國香港

關於作者

森美力 (Samiux) (網名) 是一名資訊科技安全 (Information Security, InfoSec) 愛好者，他擁有由美國 Offensive Security 發出的 OSCE (Offensive Security Certified Expert)，OSCP (Offensive Security Certified Professional) 及 OSWP (Offensive Security Wireless Professional) 專業認證。他對網絡攻擊有深入認識，了解惡意黑客的行為。他是一名黑客，但並不是惡意黑客，嚴格來說，讀者可以稱他為灰客 (Grey Hat，灰帽子)。他的格言是「未知攻，焉知防」。

他曾在警隊服務，具有多年刑事偵緝經驗，對罪犯行為心態略有研究。

他是 Linux 系統的愛好者，他喜歡使用 Ubuntu Linux。

他擁有多個活躍的資訊科技安全研究項目，例如防禦入侵系統，匿名瀏覽系統，高安全性網頁伺服器設定，「抓我吧，若果你有能力的話」系列，人功智能網頁防火牆等。他也是一名博客 (Blogger)。他閒時會編寫程式及閱讀，他更會在其滲透測試 (Penetration Testing) 實驗室中作實驗時而自得其樂。他有建設同時亦有破壞。

他的其他著作有「武裝自己 - 資安篇」及「軍事演習 - 資安篇」。

讀者可以在這裡接觸他 ：

(1) 其博客 - https://samiux.blogspot.com
(2) 其網站 - https://www.infosec-ninjas.com
(3) IRC freenode - #infosec-ninjas

關於本書

在寫作本書時，我考慮到一般的電腦書籍都因為軟件與硬件的更新，而令書中所描述的題材和內容脫節。所以我想寫一本較為長春的書籍。並且會用較為深入淺出的書寫方式去完成。

本書主要論述的是如何從認識惡意黑客網絡攻擊到認識自己的強項和弱項，而達到「知彼知己」的境地，從而做到每戰不殆。

本書對象

讀者需要具有一般資訊科技安全知識。本書是寫給那些系統管理員、網站管理員、網絡管理員、系統開發者及想在網上滑浪時倍加安心的讀者。

致謝

出書是個浩大的工程項目，在本書寫作其間，經常遇到很多困難，經過數天時間的努力才完成。借此機會感謝所有使本書能夠順利出版及提供幫助的專家及朋友。

特別感謝我女友在背後的支持。感謝我的家人和朋友，你們為我付出很多！

在此，我要感謝活躍在網絡上的資訊科技安全專家們，你們的公開文章和技巧讓我學到了很多優秀的技術。

聲明

第一章　知彼

大多數的惡意黑客視法律如無物，又或想盡辦法來逃避法律責任。他們有極高的能力來隱蔽其身份及藏身之處。

大部份的網絡攻擊大致都會經過 ：

(1) 資料搜集 (Reconnaissance) ;
(2) 掃描目標 (Scanning) ;
(3) 漏洞分析 (Vulnerability Analysis) ;
(4) 漏洞利用 (Exploit) ;
(5) 用戶提權 (Privilege Escalation) ;
(6) 後期利用 (Post Exploit)。

資料搜集

如果惡意黑客對其目標未有足夠的認識和資料，他們會進行資料搜集。資料搜集分為主動式 (Active) 和被動式 (Passive)。主動式資料搜集會在目標處作出搜索，務求得到有價值的訊息。但此等搜索方法會在目標留下大量的足跡，目標有可能察覺得到而作出防範而打草驚蛇。

至於被動式，惡意黑客會在周邊環境作出資料搜集。例如招聘廣告、接觸員工、從互聯網上的搜尋器所得等等。這樣的話，他們幾乎不會留下任何足跡在目標處。有時兩種搜集方式都會同時使用，以求得到最多有價值的訊息。搜集訊息的時間可長可短，越重要的目標所需的時間可能越長，有可能歷時數年。

惡意黑客是一群非常有耐性的敵人，他們不會放過他們的獵物，不論是垂手可得，抑或是要大費周章才能獲得到的。

掃描目標

當惡意黑客完成了資料搜集後，他們會對目標進行掃描。目的是要找出目標是正在運行那些服務 (Service) 或軟件。掃描亦有分主動式和被動式，主動式是直接向目標進行掃描，而被動式就是經過第三方作出掃描動作。

漏洞分析

當掃描完成後，惡意黑客會根據掃描所得的資料對目標進行漏洞分析。大多數的時間是分析現有已被發現的漏洞 (Vulnerability)，但有時惡意黑客會不惜公本去發掘那些零日漏洞 (0day)，目的只求達到入侵目標。

漏洞發掘和開發是需要較高的技術，所以並不是所有惡意黑客都能夠做到。除了漏洞分析外，此階段惡意黑客有可能發動社會工程 (Social Engineering) 來對付其目標。

漏洞利用

一但發現目標正在運行或使用有漏洞的服務或軟件，惡意黑客就會進行漏洞利用 (Exploit)，作出入侵行動。如果目標沒有在防禦措施的保護下，如防毒軟件、防火牆等等，惡意黑客就會如入無人之境，輕鬆自在地進行入侵。

若果遇有防禦措施，惡意黑客會想盡辦法去繞過其保護，又或直接關掉其保護機制來作進一步的入侵。

用戶提權

入侵後，若果有漏洞的服務或軟件不是以管理員身份運行的話，惡意黑客就會利用系統錯誤的設置，又或是利用系統的漏洞進行提升權限，令其得到系統的最高權限。有時並不需要權限提升也可以完成任務。又或者利用社會工程來得到所需權限。

後期利用

當完成入侵行動後，惡意黑客會留下後門 (Backdoor)，以便下次再來時不必大費周章。他們更會在系統內清除所有足跡，以防洩露行蹤。有時惡意黑客會替目標修復漏洞，以防被其他惡意黑客所利用。

被入侵後的目標可以作很多用途，例如作為跳板用作其他入侵行動，又或用來發報不良訊息，如兒童色情多媒體等等。如果入侵後的目標是最終的獵物，惡意黑客可以獲得獵物的所有資料及檔案，並能控制整個系統。亦可進而入侵網內其他系統。

第二章　知己

開發者

很多開發的編程人員 (Programmer) 會用較為複雜又省時省力的程序和邏輯去完成工作。在他們來說,這是精湛技術和效率的表現。但是，一旦在程序上或邏輯上出現一些連開發者都察覺不到的問題，又或在除錯 (Debugging) 時出現困難，兩者都可能成為被惡意黑客利用的漏洞。

又有些編程人員不知道如何編寫安全的代碼 (Code)，他們更不知道有些編程技巧或程序有安全問題。

要解決這個問題是要從安全的編程訓練開始。有時簡單就是美！

管理員

有些系統管理員、網站管理員和網絡管理員對其要使用的技術不甚了解，有些地方不知道如何設定或安排，便隨意地參考網上的所謂教學 (Tutorial 或 Guide) 來設定其要管理的系統。可是那些教學在資訊科技安全領域上良莠不齊，容易做成不安全的設定，令其系統面對安全的風險。

又有些管理員不求甚解，將其認為安全的設定用在其要管理的系統上。要解決這些問題，首先要管理員明白錯誤的設定所帶來的風險，進而了解其要管理的系統的技術上問題，學習如何安全地設定其系統。

普通用家

大部份的普通用家都會在自己家裏建立或者租用伺服器。他們大多數沒有資訊科技安全知識而做成系統在安全上的高風險。要他們學習資訊科技安全技術有一定的難度。所以，普通用家是資訊科技安全的一大缺口。要他們明白和認識資訊科技安全不是三言兩語便能解決的問題。

此外，普通用家是非常容易墮入社會工程陷阱，所以長期資訊科技安全教育是少不了的。

經常更新

系統更新有功能更新和安全更新之分。所有系統不論是電腦系統、路由器、流動設備、防毒軟件特徵或嵌入式系統 (Embedded System)，都應該經常更新。不可以給惡意黑客有機可乘。

防毒軟件

雖然現在防毒軟件十分流行，但仍然會有人認為防毒軟件是多餘之物。尤以類 Unix 系統的使用者，如 Linux、macOS 及 BSD 系統，他們認為類 Unix 系統在設計上是非常安全，黑客無可能用惡意軟件入侵。加上他們認為大部份的類 Unix 使用者都是電腦專家，不會輕易受到黑客攻擊。

但事實並非如此，大多數被入侵的系統都是類 Unix 系統。雖然防毒軟件並不是靈丹妙藥，而且它具有一定的限制性，但它仍然有其一定的防禦能力。正如第一章所述，防毒軟件可增加入侵者的門檻。

所以，如果情況許可的話，我建議盡可能使用防毒軟件或防惡意軟件。

防火牆

防火牆，現在有雲端網頁防火牆、網頁防火牆 (Web Application Firewall, WAF) 及普通防火牆之分。基本上，雲端網頁防火牆和網頁防火牆是一樣的，分別在於是在雲端上與否。至於普通防火牆，大部份人都對其有所認識及樂意使用。

大部份人都不知道現在 (直至截稿時) 的雲端網頁防火牆在設計上有一定的限制，就是不能在加密的情況下正常運作。如果那些加密了的網站在雲端網頁防火牆的保護下，遇到黑客精心設計的攻擊，其保護效果就會蕩然無存。

所以不要太過信賴雲端網頁防火牆，最有效防禦黑客入侵網站的方法就是網站的安全編程，正如「開發者」一節所提到的。

防禦入侵系統

基本上，防禦入侵系統 (Intrusion Detection and Prevention System, IDPS) 並不能阻擋零日漏洞。它的運作與防毒軟件十分相似，它們都是利用漏洞特徵和病毒特徵運作。

防禦入侵系統大多是用來保護一些不能及時使用安全更新的有漏洞系統。在可能的情況下，那些有漏洞的系統應該盡快更新。

我們不能恃着有防禦入侵系統就不對系統進行安全更新。這是一個大錯特錯的觀念。再者，我們應該時常保持防禦入侵系統的漏洞特徵在最新版本，目的是阻擋最新發現的漏洞利用。

另外，基本上防禦入侵系統和防火牆並不能處理已經加密了的流量。所以，惡意黑客經常會使用加密了的方式去進行入侵行動來窺避各式各樣的保護機制。

第三章　兵者，詭道也

孫子兵法有云 ：「兵者，詭道也。故能而示之不能，用而示之不用，近而示之遠，遠而示之近。」

在惡意黑客網絡攻防方面，如果我們可以誤導惡意黑客，使其認為我們不存在、沒有攻擊面 (Attack Vector) 或堅不可摧的話，我們便能延遲或者甚至可以防止被入侵。

如果我們可以在惡意黑客在進行資料搜集和掃描行動時作出有效的誤導的話，惡意黑客就不能獲得有效的資訊來作進一步的攻擊。

又如果我們可以阻擋惡意黑客所使用的常用工具，加上將所有疆屍網絡 (Botnet)、已被入侵的系統 (Compromised) 和具有惡意企圖紀錄的網絡地址列入黑名單內，我們的系統被攻擊的可能性就會大大減少。

這會看似遙不可及，但現實是有這樣的防禦系統的。如有興趣，可參閱附件二。

附件一　基本概念

甚麼是惡意軟件?
惡意軟件 (Malware) 具有不良企圖的軟件。例如，病毒 (Virus)，木馬 (Trojan)，蠕蟲 (Worm)，勒索軟件 (Ransomware) 等。其出現形態包括執行檔或腳本 (Script)，如 JavaScript。

病毒有自我複製及感染其他檔案的能力。木馬就是所謂的後門 (Backdoor)。蠕蟲具有滲透能力，即會攻擊下一個目標。勒索軟件可能會具備以上所有特徵及加上將受害者的檔案加密，並要求贖金來解密。

當下幾乎所有網站都有使用 JavaScript 來製作互動網頁。JavaScript 是在瀏覽者的電腦上運行。若果網站被騎劫或者該網站由惡意黑客所建立，在其網頁植入惡意的 JavaScript 的話，受害者多數在不知情的情況下受到感染而被入侵。

甚麼是社會工程？
社會工程 (Social Engineering) 是一種欺騙的手段和技巧。出現的形態可以千變萬化，可以是經電話、電郵、連結、網站及下載等。我們經常聽到的「釣魚」 (Phishing)，就是其中一種。誘使受害者作出或不作出某種行為，而達到目的。

甚麼是中間人攻擊？
中間人攻擊 (Man-In-The-Middle Attack) 是受害者的通訊被脅持，其通訊被脅持者篡改或監聽 (Sniffing)。有時已加密的通訊亦可以被脅持者篡改或監聽。

有時可以在受害者下載或上載檔案時，植入惡意軟件。這的確是防不勝防。

甚麼是漏洞？
漏洞 (Vulnerability) 是指程式設計時在邏輯上或編程上出錯。這可以看作是一個「臭蟲」(Bug)。不是所有臭蟲都是漏洞，不是所有的漏洞都可以被利用 (Exploit)。可被利用的漏洞是可以入侵受害者的系統。

通常漏洞可以經更新而修復。但是在某些情況下，有些系統在有更新的情況下，也不能作出更新，例如若果更新了，系統就會崩潰。

甚麼是密碼強度？
從前的密碼長度建議是八個位，但是因為現今的硬件運算能力非常強大，八個位長度的密碼可以在少於十五分鐘內被破解。

所以我現時建議至少十六個位的長度，其組合包括大細楷英文字母，數目字及標點符號。而且其組合不能有意思或可以被推算得到。

因為這麼長的密碼是非常難記憶的，所以讀者應該要有密碼策略 (Password Policy)。再者，盡可能不要重用密碼。因為只要密碼被洩漏，你的所有賬號就會全軍覆沒。

甚麼是保安設備？
常見的保安設備有防毒軟件及防火牆。但尚有統一威脅管理系統 (Unified Threat Management System, UTM) 及防禦入侵系統 (Intrusion Detection and Prevention System, IDPS) 等。

現在的統一威脅管理系統和防禦入侵系統十分相似。所以在選購時要清楚了解產品的特性和自己的需求。現在更流行一種叫做下世代防火牆 (Next-Generation Firewall)，其實它與統一威脅管理系統和防禦入侵系統相當近似。

甚麼是備份？
備份 (Backup) 是將你的有價值的檔案做一個複製品，並安置於一個安全地方。備份有分日、月、年。而當中亦有雙單日，雙單月，雙單年之分。以防數據流失，最好有超過一個複製品。

甚麼是黑客？
黑客 (Hacker) 一般是指技術精湛的人，能令設備做出一些不在設計情況之下運作。

在資訊科技安全領域下，黑客是指一個具有精湛電腦技術的人，能使電腦或其程式於不在其設計的情況下運作。在我等來說，黑客有分黑帽子

(Black Hat)，白帽子 (White Hat)，灰帽子 (Grey Hat) 及腳本小子 (Script Kiddies)。

黑帽子是指所謂駭客，他們是作奸犯科之流。

白帽子是指資訊科技安全專家或研究員，他們測試系統漏洞，並公報結果給有關開發人員或機構。

灰帽子也是資訊科技安全專家或研究員，他們也測試系統漏洞，但他們大多數不會向有關開發人員或機構公報其發現，他們會直接披露 (Full Disclosure)。他們多數走在法律邊緣，但並沒有惡意。

至於腳本小子，他們並不是資訊科技界中人。他們會利用黑客工具作樂或者作惡。

附件二　牛角包

牛角包 (Croissants) 是一個設計十分獨特的防禦入侵系統。她是一個開源項目，由我獨自開發，她是完全免費使用的。她獨特之處在於她能夠識別惡意黑客的企圖，進而作出攔截反應。

雖然設計簡單，沒有華麗的使用介面，但是她的效能非常高，能處理 1000 Mbps 或以上流量。她的低延遲特性，對綫上遊戲的影響減至最少。適合用於個人，家庭，小型企業等。

她近似於統一威脅管理系統和下世代防火牆。她具有抵擋病毒，偵測掃描，堵塞漏洞等等功能。

硬件基本要求 ：

(1) 多核心 x86 處理器
(2) 具有 AVX2 功能的核心
(3) 8 GB 記憶體
(4) 128 GB 硬碟
(5) 3 個 1000 MB 網絡界面

詳情請瀏覽我的個人網站 (https://www.infosec-ninjas.com)，是英文版本的。

全書完